UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,515	07/25/2003	Lee E. Cannon	IGT1P551/P-834	3255

22434 7590 04/04/2008

BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
HOEL, MATTHEW D	
ART UNIT	**PAPER NUMBER**
3714	

MAIL DATE	DELIVERY MODE
04/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/627,515	CANNON, LEE E.	
	Examiner	Art Unit	
	Matthew D. Hoel	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,23,24 and 26-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,23,24 and 26-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1-36,38-40, and 42-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martinek et al. (WO 031045519, entered as FPL 8-23-2007), "Martinek" in view of Rackman (US 4,670,857), "Rackman".

Claims 1, 19, 32, 38, 39, 42 and 46: Martinek discloses an apparatus:

• a display unit(pg. 24, line 27);

• a value input device(pg. 24, line 27);

• a controller operatively coupled to said display unit and said value input device, said controller comprising a processor and a memory operatively coupled to said processor (pg. 25, lines 10, 11 and lines 27-31),

• said controller being programmed to receive downloadable gaming data from a data storage device external to said gaming apparatus(pg. 27, lines 11-19);

• said controller being programmed to receive encrypted gaming data from said data storage device, said encrypted gaming data having been generated by performing a hash function on gaming data to form a first message digest and by encrypting said first message digest utilizing a private encryption key of a gaming data authoring organization and a private encryption key of a gaming regulatory organization(pg. 27, line 13- pg. 28, line 7);

• said controller being programmed to decrypt said encrypted gaming data utilizing a public encryption key of said gaming data authoring organization and a public encryption key of said gaming regulatory organization to form a decrypted message digest(pg. 29, lines 21-25);

• said controller being programmed to perform a hash function on said downloadable gaming data to generate a second message digest(pg. 27, lines 30-33 and pg. 30, lines 18-25); and

• said controller being programmed to compare said decrypted message digest with said second message digest to determine if said downloadable gaming data is authorized(pg. 27, line 30-33 and pg. 30, lines 18-25).

4. Martinek does not disclose double encryption as claimed. Instead, Martinek teaches single encryption (pg. 27, line 13 - pg. 28, line 7) and authentication from both a regulatory agency (pg. 30, lines 26-28) and a game code manufacturer (pg. 31, lines 1-

2). In an analogous game security reference, Rackman (col. 6, lines 1-13) teaches doubly encrypting the message to insure both privacy and authentication.

5. One of ordinary skill in the art would have seen the benefit of double encryption because it allows the receiver to authenticate the transmitter and the transmitter to allow only the receiver to decrypt the message. Therefore, it would have been obvious to one or ordinary skill in the art at the time of the instant invention to modify Martinek with double encryption as taught by Rackman to insure both privacy and authentication.

6. An updated review of the prior art leads the examiner to believe that the modification would have been within the knowledge and skill of one of ordinary skill in the art at the time the invention was made. Figs. 12A,B of U.S. patent 6,866,586 B2 (published before applicants' priority date as 2002/00077178 A1) shows a double-encryption method in which two parties encrypt a message with their respective keys, resulting in double encryption, before the message is forwarded to a third party. In Fig. 12A, step 1208, of '178, the message is encrypted with A's public key and the clearinghouse's private key. In step 1224, the message is encrypted with B's public key and the clearinghouse's private key before being transmitted to B. Figs. 1 and 2 of WO 01/06691 A1 (PCT/US00/19944, entered as FPL 8-23-2007) also show double encryption involving keys from two parties. In step 116 of Fig. 1, the message is first encrypted with a user's public key. In step 124 of Fig. 1, the message is again encrypted with the network site's private key, resulting in a doubly encrypted message with keys from two parties. O'Reilly's "Practical UNIX & Internet Security," (entered as NPL 8-23-2007) chapter 6 on cryptography, by Garfinkel, et al., 2nd ed., Apr. 1996, ISBN

1-56592-148-8, found at http://www.unix.org.ua/orelly/networking/puis/index.htm, outlines double DES encryption on Page 8 in section 6.4.5.1. The message is first encrypted with one key, then another. This requires an attacker to check 2^{112} keys instead of 2^{57} keys. Section 6.4.5.2 takes this a step further with triple DES encryption in which the message is successively encoded with key1, key2, and key3 and then successively decoded by key3, key2, and key1. Since multiple (including double) encrypting and double encrypting using separate keys from separate entities are known in the art generally, would have been will within the motivation and skill level of an ordinary practitioner to encrypt a message twice using private keys from two respective entities and to decrypt the message upon reception using two public keys from the two respective entities. A review of the Martinek specification provides some motivation for this modification. 33:12-20 discusses encrypting communications with digital signatures from the Navada Gaming Commission to ensure that the downloaded coded has been approved by the Commission. 30:26-31:2 outlines embodiments in which the code is digitally signed by the developer or the Commission. Rather than teaching away, one of ordinary skill in the art could use double encryption so that the downloaded code could be encrypted by both, which would be better than either embodiment separately. Indeed, 30:30-33 suggests providing security to both the game operator and the Commission. 24:5-22 of Martinek also discusses DES encryption and mentions that it is intended that Martinek's application could be used with other authentication methods expected to be developed in the future, so Martinek would have been amenable to the DES multiple encryption of O'Reilly or the double encryption of the Rackman reference;

this suggestion makes it obvious to try the combination in light of KSR (550 U.S. (2007) at 17): "When there is a design need or a market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. In that instance the fact that a combination was obvious to try might show that it was obvious under § 103."

7. Claim 2: Martinek discloses an apparatus wherein said data storage device comprises a portable data storage medium on which said downloadable data was stored when said portable data storage medium was at a location external to said gaming apparatus and wherein said portable data storage medium is physically moved so that it is operatively coupled to said gaming apparatus in order to transfer said downloadable gaming data to said controller (pg. 26, lines 19-30).

8. Claim 3: Martinek discloses an apparatus wherein-said controller is programmed to receive downloadable gaming data that comprises substantially all gaming data that is necessary to facilitate play of a casino game (pg. 26, lines 15-18).

9. Claim 4: Martinek does not disclose an apparatus wherein said controller is programmed to receive from said data storage device encrypted gaming data that was generated by triply encrypting said first message digest utilizing said private encryption key of said gaming data authoring organization, said private encryption key of said gaming regulatory organization, and a private encryption key of a

casino, and wherein said controller is programmed to triply decrypt said encrypted gaming data utilizing said public encryption key of said gaming data authoring organization, said public encryption key of said gaming regulatory organization, and a public encryption key of said casino to form said decrypted message digest. Instead, Martinek teaches single encryption (pg. 27, line 13 - pg. 28, line 7) and authentication from a regulatory agency (pg. 30, lines 26-28), a game code manufacturer (pg. 31, lines 1-2) and casinos (pg. 3, lines 24-33). In an analogous game authentication reference, Rackman teaches doubly encrypting the message to insure both privacy and authentication (col. 6, lines 1-13). It would have been obvious to one of • ordinary skill in the art to add a third encryption to increase the layers of encryption and therefore increase security. One would have seen the benefit of the third layer of encryption supported by the casino, game regulatory authority and/or game code manufacturers because casino managementand the governmental regulatory agencies are very concerned with electronic intruders tapping into the casino communication network and manipulating any player terminal, including a slot machine, to fraudulently declare a jackpot. Therefore, it would have been obvious to one or ordinary skill in the art at the time of the instant invention to modify Martinek as modified by Rackman with a third encryption to provide casinos and regulatory agencies (and game code manufacturers) to insure privacy and authentication; thereby preventing tampering and fraudulent jackpots.

10. Claim 5: Martinek discloses an apparatus wherein said gaming system additionally comprises a central computer operatively coupled to each of said gaming

apparatuses, said central computer comprising a memory, and wherein said controller is programmed to receive said downloadable gaming data from said memory of said central computer (pg. 11, lines 21-33).

11. Claim 23: Martinek discloses an apparatus wherein said display unit comprises a video display unit that is capable of generating video images(pg. 24, line 27).

12. Claim 24: Martinek discloses an apparatus, wherein said controller is programmed to cause a video image comprising an image of at least five playing cards to be displayed if said game comprises video poker, wherein said controller is programmed to cause a video image comprising an image of a plurality of simulated slot machine reels to be displayed if said game comprises video slots, wherein said controller is programmed to cause a video image comprising an image of a plurality of playing cards to be displayed if said game comprises video blackjack, wherein said controller is programmed to cause a video image comprising an image of a plurality of keno numbers to be displayed if said game comprises video keno, wherein said controller is programmed to cause a video image comprising an image of a bingo grid to be displayed if said game comprises video bingo(pg. 2, lines 13-30 and pg. 34, lines 23-33).

13. Claim 26: Martinek discloses an apparatus, comprising:

• a display unit (pg. 24, line 27);

• a value input device (pg. 24, line 27);

• a controller operatively coupled to said display unit and said value input device, said controller comprising a processor and a memory operatively coupled to said

processor, said controller being programmed to receive downloadable gaming data from a data storage device external to said gaming apparatus(pg. 25, lines 10, 11 and lines 27-31);

• said controller being programmed to receive encrypted gaming data from said data storage device, said encrypted gaming data having been generated by performing a data-abbreviating function on gaming data to form first abbreviated gaming data and by doubly encrypting said first abbreviated gaming data utilizing an encryption key of a gaming data authoring organization and an encryption key of a gaming regulatory organization (pg. 8, lines 13-27);

• said controller being programmed to decrypt said encrypted gaming data utilizing an encryption key of said gaming data authoring organization and an encryption key of said gaming regulatory organization to form decrypted gaming data(pg. 27, line 13 - pg. 28, line 7);

• said controller being programmed to perform a data-abbreviating function on said downloadable gaming data to generate second abbreviated gaming data(pg. 8, lines 13-27); and

• said controller being programmed to compare said decrypted gaming data with said second abbreviated gaming data to determine if said downloadable gaming data is authorized(pg. 8, lines 13-27).

14. Martinek does not disclose double encryption as claimed. Instead, Martinek teaches single encryption (pg. 27, line 13 - pg. 28, line 7). In an analogous game security reference, Rackman (col. 6, lines 1-13) teaches doubly encrypting the message

to insure both privacy and authentication. One of ordinary skill in the art would have seen the benefit of double encryption because it allows the receiver to authenticate the transmitter and the transmitter to allow only the receiver to decrypt the message. Therefore, it would have been obvious to one or ordinary skill in the art at the time of the instant invention to modify Martinek with double encryption as taught by Rackman to insure both privacy and authentication.

15. Claim 27: Martinek discloses an apparatus wherein said controller is programmed • to cause a video image comprising an image of at least five playing cards to be displayed if said game comprises video poker, wherein said controller is programmed to cause a video image comprising an image of a plurality of simulated slot machine reels to be displayed if said game comprises video slots, wherein said controller is programmed to cause a video image comprising an image of a plurality of playing cards to be displayed if said game comprises video blackjack, wherein said controller is programmed to cause a video image comprising an image of a plurality of keno numbers to be displayed if said game comprises video keno, wherein said controller is programmed to cause a video image comprising an image of a bingo grid to be displayed if said game comprises video bingo (pg. 2, lines 13-30 and pg. 34, lines 23- 33).

16. Claim 28: Martinek discloses an apparatus wherein said data storage device comprises a computer located at a location remote from said gaming apparatus and wherein said controller is programmed to receive said downloadable gaming data from said computer (pg. 11, lines 21-33).

17. Claim 29: Martinek discloses an apparatus wherein said data storage device comprises a portable data storage medium on which said downloadable data was stored when said portable data storage medium was at a location external to said gaming apparatus and wherein said portable data Storage medium is physically moved so that it is operatively coupled to said gaming apparatus in order to transfer said downloadable gaming data to said controller(pg. 26, lines 19-30).

18. Claim 30: Martinek discloses an apparatus wherein said controller is programmed

to receive said encrypted gaming data along with said downloadable gaming data(pg. 27-29).

19. Claim 31: Martinek discloses an apparatus wherein said controller is programmed to receive said encryption key of said gaming data authoring organization and said encryption key of said gaming regulatory organization(pg. 30, lines 26-30).

Response to Arguments

20. Applicant's arguments filed Dec. 26th, 2007 have been fully considered but they are not persuasive. The examiner's previous "Response to Arguments" and advisory action comments are incorporated by reference. An updated review of the prior art leads the examiner to believe that the modification would have been within the knowledge and skill of one of ordinary skill in the art at the time the invention was made. Figs. 12A,B of U.S. patent 6,866,586 B2 (published before applicants' priority date as 2002/00077178 A1) shows a double-encryption method in which two parties encrypt a

message with their respective keys, resulting in double encryption, before the message is forwarded to a third party. In Fig. 12A, step 1208, of '178, the message is encrypted with A's public key and the clearinghouse's private key. In step 1224, the message is encrypted with B's public key and the clearinghouse's private key before being transmitted to B. Figs. 1 and 2 of WO 01/06691 A1 (PCT/US00/19944) also show double encryption involving keys from two parties. In step 116 of Fig. 1, the message is first encrypted with a user's public key. In step 124 of Fig. 1, the message is again encrypted with the network site's private key, resulting in a doubly encrypted message with keys from two parties. O'Reilly's "Practical UNIX & Internet Security," (entered as NPL on 8-23-2007) chapter 6 on cryptography, by Garfinkel, et al., 2nd ed., Apr. 1996, ISBN 1-56592-148-8, found at http://www.unix.org.ua/orelly/networking/puis/index.htm, outlines double DES encryption on Page 8 in section 6.4.5.1. The message is first encrypted with one key, then another. This requires an attacker to check 2^{112} keys instead of 2^{57} keys. Section 6.4.5.2 takes this a step further with triple DES encryption in which the message is successively encoded with key1, key2, and key3 and then successively decoded by key3, key2, and key1. Since multiple (including double) encrypting and double encrypting using separate keys from separate entities are known in the art generally, would have been will within the motivation and skill level of an ordinary practitioner to encrypt a message twice using private keys from two respective entities and to decrypt the message upon reception using two public keys from the two respective entities. A review of the Martinek specification provides some motivation for this modification. 33:12-20 discusses encrypting communications with digital signatures

from the Navada Gaming Commission to ensure that the downloaded coded has been approved by the Commission. 30:26-31:2 outlines embodiments in which the code is digitally signed by the developer or the Commission. Rather than teaching away, one of ordinary skill in the art could use double encryption so that the downloaded code could be encrypted by both, which would be better than either embodiment separately. Indeed, 30:30-33 suggests providing security to both the game operator and the Commission. 24:5-22 of Martinek also discusses DES encryption and mentions that it is intended that Martinek's application could be used with other authentication methods expected to be developed in the future, so Martinek would have been amenable to the DES multiple encryption of O'Reilly or the double encryption of the Rackman reference; this suggestion makes it obvious to try the combination in light of KSR (550 U.S. (2007) at 17): "When there is a design need or a market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. In that instance the fact that a combination was obvious to try might show that it was obvious under § 103."

21. The applicants appear to be conflating novelty with non-obviousness. The examiner explained in the last action how applying the dual-agency approval of Martinek and the double encryption of Rackman to create double encryption using first the private key of one agency then the private key of another agency, which is doubly decrypted upon receipt with the public keys of both agencies. The claimed limitation is

merely a superposition of known encryption techniques and is obvious for the reasons outlined above; the limitation is novel but not non-obvious. Rackman in Cols. 5 and 6 teaches double encryption. Rackman also teaches that the message is encrypted with the sender's private key and decrypted with the sender's public key. This combined with Martinek's dual agency approval results in the claimed first encryption with a first agency's (sender's) private key, then encryption with a second agency's (sender's) private key, then the receiver doubly decrypting the message with both senders' public keys. Being discrete mathematics, encryption is predictable with every expectation of success when the two techniques are applied together. One of ordinary skill in the art at the time the invention was made would have wanted the receiving gaming machine to 1) know that the message authentically game from the gaming manufacturer and 2) was authentically approved by the gaming authority before being sent to the gaming device over the network. Only the manufacturer and gaming authority would know their respective private keys, ensuring security in this regard. The gaming device would have the public keys for both entities, so it would know that the respective entities properly encoded the message with their respective private keys. The public keys allow anybody to authentically know who the sender is without knowing the sender's private key. The examiner also points the applicants to Gressel, et al., U.S. patent 5,664,017 A, which teaches two separate agencies double-encrypting a message (11:23-27, each agency separately encoding the message with their respective public keys) and double-decrypting the message (15:16-37, each agency decrypting the message with their respective private keys). Schneier, et al. in U.S. patent 6,099,408 A, Fig. 16, teaches

encrypting with a private key and decrypting with a public key in a gaming application. The claimed invention would thus simply be a duplication of structure where the claimed limitation is created by first encrypting with two separate private keys and then decrypting upon receipt with those two private keys' respective public keys (MPEP 2144.04(VI)(B)). While the limitation is novel, it would have been well within the skill and motivation of one of ordinary skill in the gaming art to make. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The examiner respectfully disagrees with the applicants as to the claims' condition for allowance.

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew D. Hoel whose telephone number is (571)272-5961. The examiner can normally be reached on Mon. to Fri., 8:00 A.M. to 4:30 P.M.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert E. Pezzuto can be reached on (571) 272-6996. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

24. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Matthew D. Hoel
Patent Examiner
AU 3714

/Robert E. Pezzuto/
Supervisory Patent Examiner
Art Unit 3714

/M. D. H./
Examiner, Art Unit 3714